

**Problem set 2***April 23, 2013*

Due: May 7

- Please submit the handout in class.
- Write clearly and shortly using sub claims if needed. The emphasize in most questions is on the proofs (no much point is writing a “solution” w/o proving its correctness)
- For Latex users, a solution example can be found in the course web site.
- In case you work in (small) groups, please write the id list of your partners in the solution file. I stress that each student should write his solution by *himself* (joint effort is only allowed in the “thinking phase”)
- The notation we use appear in the first lecture ([www.cs.tau.ac.il/~iftachh/Courses/FOC/Fall11/Slides/OWF.pdf](http://www.cs.tau.ac.il/~iftachh/Courses/FOC/Fall11/Slides/OWF.pdf)), section “Notation”

**Exe 1, non-adaptive PRF (10 points).**

A function family is a *non-adaptive* PRF, if it is a PRF according to the definition given in class, but its security should only holds against *non-adaptive* distinguishers: distinguishers that choose all queries to the oracle *before* making the first query (alternatively, they make all there queries at once).

1. Prove that an (adaptive) PRF is also a non-adaptive one
2. Assume OWF exists, prove there exist a non-adaptive PRF that is *not* an (adaptive) PRF

**Exe 2, Weak PRFs (10 points).** A function family is a *weak* PRF, if it is a non-adaptive PRF according to the above definition, but its security should only holds against (non-adaptive) distinguishers who choose their queries *uniformly and independently* from the set of all possible queries.

1. Assume OWF exists, prove there exists a weak PRF that is not a non-adaptive PRF

**Exe 3. PRF to PRG. (10 points)** Show that if there exist “not trivial” pseudorandom functions ensemble  $\mathcal{F} = \{\mathcal{F}_n\}$  (i.e., the domain of  $f \in \mathcal{F}_n$ , is  $\{0, 1\}^{\ell(n)}$  for a polynomial-time computable  $\ell(n) \in \omega(\log n)$ ), then there exist pseudorandom generators.

Note that there are no assumptions on the output length of the functions. Also don't go through one-way functions (unless you like to fully prove that one-way functions imply pseudorandom generators...)

**Exe 4. Constructing pairwise-independent function family. (10 points)** Recall that a function family  $\mathcal{H} = \{h : \{0, 1\}^n \rightarrow \{0, 1\}^m\}$  is *pairwise independent*, if for any for any  $x \neq x' \in \{0, 1\}^n$  it holds that

$$\Pr_{h \leftarrow \mathcal{H}}[h(x) = h(x')] = 2^{-m}$$

(That is, the probability that two fixed points in the domain collide under  $h$  is exactly the same as if  $h$  were a truly random function from  $\{0, 1\}^n$  to  $\{0, 1\}^m$ .)

There are many combinatorial constructions of efficient ensembles of pairwise independent hash functions with short description, in the following we consider one such a family.

Let  $A_{n \times m}$  be the set of all  $n \times m$  binary matrices. Show that the family  $\mathcal{H} := \{h_{A,b} : A \in A_{n \times m}, b \in \{0, 1\}^m\}$ , where  $h_{A,b}(x) \equiv Ax + b \pmod{2}$ , is pairwise independent.

**Exe 4, PRF domain extension.** Let  $\mathcal{F} = \{\mathcal{F}_n = \{f : \{0, 1\}^n \mapsto \{0, 1\}^n\}\}_{n \in \mathbb{N}}$  be a PRF, and let  $\mathcal{H} = \{\mathcal{H}_n = \{h : \{0, 1\}^{2n} \mapsto \{0, 1\}^n\}\}_{n \in \mathbb{N}}$  be an efficient pairwise-independent function family.<sup>1</sup> We would like to prove that the function family ensemble  $\mathcal{F} \circ \mathcal{H} =$

---

<sup>1</sup>Namely, the family  $\mathcal{H}_n$ , for each  $n \in \mathbb{N}$ , is pairwise independent.

$\{\mathcal{F}_n \circ \mathcal{H}_n = \{f \circ h: f \in \mathcal{F}_n, h \in \mathcal{H}_n\}\}_{n \in \mathbb{N}}$  is a PRF mapping strings of length  $2n$  to string of length  $n$ .<sup>2</sup>

(10 points) Prove that function family ensemble  $\{\Pi_n \circ \mathcal{H}_n\}_{n \in \mathbb{N}}$  is computationally (actually, also statistically) indistinguishable from  $\{\Pi_{n,2n}\}$ .

(10 points) Use the above to prove that  $\mathcal{F} \circ \mathcal{H}$  is a PRF.

---

<sup>2</sup>The symbol  $\circ$  stands for function concatenation, e.g.,  $f \circ h(x) = f(h(x))$ .